POLÍTICA DE FIRMA ELECTRÓNICA

Este documento tiene por objeto establecer las condiciones generales de seguridad, de organización y técnicas para determinar cómo se generan, verifican y gestionan las firmas electrónicas en Enresa, incluyendo las características exigibles a los certificados de firma.

Alcance y aplicación

Esta Política aplica a todo el personal de Enresa y a todas las personas físicas y jurídicas que se relacionen con la compañía a través de medios electrónicos. Así mismo, aplica en el marco de interoperabilidad de Enresa con las Administraciones Públicas, dentro de su ámbito de actuación, para el uso de la firma electrónica de transmisiones de datos.

La Política es de aplicación tanto a las firmas basadas en certificados como a los sellos electrónicos.

Uso de la firma y los sellos electrónicos

La firma electrónica, como mecanismo para la seguridad de la información, podrá aplicarse en:

- La firma de transmisiones de datos, como herramienta para proporcionar seguridad al intercambio de datos, garantizando la autenticación de los actores involucrados en el proceso, la integridad del contenido del mensaje de datos enviado y el no repudio de los mensajes en una comunicación telemática.
- La firma de contenido, como herramienta para garantizar la autenticidad, integridad y no repudio de aquel. Equivale, en el entorno electrónico, a la firma manuscrita tradicional.

En caso de transmisión de un contenido firmado, tanto el contenido como su firma irán anexos a la transmisión, la cual, a su vez, podría ir firmada. Así, ambos usos de la firma son compatibles, pudiéndose utilizar de forma simultánea.

Adhesión a la Política de Firma Electrónica y de Certificados de la Administración General del Estado.

Considerando el marco legal que regula la firma electrónica y asumiendo como propio parte del contenido de la Política de Firma Electrónica y Certificados de la A.G.E., se establecen las directrices y obligaciones de todos los actores involucrados en el proceso de firma, con el objetivo de determinar la validez de la firma electrónica basada en certificados para una transacción en particular, especificando la información que deberá incluir el firmante en el proceso de generación de firma y la información que deberá comprobar el verificador en el proceso de su validación.

La Administración General del Estado dispone de una política de firma electrónica y de certificados (BOE del 13 de diciembre de 2012) que responde en parte a las necesidades que Enresa tiene relacionadas con la administración electrónica. Por su parte, Enresa desea

alinearse con la Norma Técnica de Interoperabilidad de Política de Firma y Sellos Electrónicos y de Certificados de la Administración, por lo que incorpora a su propia política las siguientes reglas:

1. Reglas comunes para el firmante de una firma electrónica:

1.1 Formatos admitidos de firma electrónica:

El formato de los documentos electrónicos con firma electrónica avanzada, aplicada mediante los certificados electrónicos admitidos por Enresa se deberá ajustar a las especificaciones de los estándares europeos relativos a los formatos de firma electrónica. Los formatos para la firma electrónica de contenido se ajustarán a la «Decisión de Ejecución UE 2015/1506» o la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) 910/2014.

La firma electrónica de transmisiones de datos estará basada en estándares recogidos en la Norma Técnica de Interoperabilidad de Catálogo de Estándares.
Enresa empleará los formatos admitidos en la Política de Firma Electrónica y de Certificados de la Administración General del Estado según los siguientes **criterios**:

- El uso del formato PDF con firma electrónica con formato mínimo PAdES-BES para todas las firmas electrónicas de contenidos que tengan como destinatarios a ciudadanos u otras administraciones públicas, salvo restricciones de formato o por la utilización de otros estándares de interoperabilidad ya establecidos.
- Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, se deberán utilizar firmas longevas mediante las que se añadirá información del estado del certificado asociado incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Así mismo se aplicarán en Enresa el certificado de sello electrónico y los perfiles básicos para garantizar la interoperabilidad de los certificados de personas físicas, personas jurídicas y entidades sin personalidad jurídica de acuerdo con la Política de Firma Electrónica y de Certificados de la AGE.

1.2. Creación de firma electrónica

Las plataformas que presten el servicio de creación de firma electrónica proporcionarán las funcionalidades necesarias para soportar un proceso de creación de firmas basado en los puntos que se especifican en el apartado 2.7 "Creación de la firma electrónica" de la Política de firma electrónica de la AGE.
El personal de Enresa en el ejercicio de sus funciones y para la forma de contenidos en fichero hará uso de los certificados cualificados corporativos de pertenencia a entidad (o de representante en los casos que sea de aplicación) que Enresa proporciona a través de un prestador de servicios de confianza cualificado. La herramienta para la firma será la aplicación realizada por el Ministerio de Hacienda y Administraciones Públicas "Autofirma" o el visor de archivos pdf que use como software corporativo Enresa.
El prestador de servicios de confianza cualificado que proporcione los certificados a utilizar en la organización expedirá los certificados bajo una Declaración de Prácticas de Certificación, Política de Certificación o de Firma Electrónica, admitida conforme la presente Política de firma electrónica de Enresa y en cumplimiento de la normativa vigente de aplicación, y así se identificará en el atributo correspondiente de las propiedades de la firma.

1.3. Algoritmos criptográficos que usar

La herramienta de firma tendrá en consideración las reglas de uso de algoritmos que se indican en la Política de firma electrónica de la AGE, destacando la necesidad de seguir las recomendaciones expresadas por el Centro Criptológico Nacional para garantizar el cumplimiento del Esquema Nacional de Seguridad, a través de las guías:

- CCN-STIC 405 "Algoritmos y parámetros de firma electrónica"
- CCN-STIC 807 "Criptología de empleo en el ENS"
- CCN-STIC 221 "Mecanismos criptográficos autorizados por el CCN"

1.4. Verificación de la firma electrónica.

El verificador puede utilizar cualquier método para verificar la firma creada según la presente política. Las condiciones mínimas que se deberán producir para validar la firma serán las siguientes:

1. Garantía de que la firma es válida para el fichero específico que está firmado.
2. Validez de los certificados en el momento en que se produjo la firma, si los servicios de los prestadores facilitan los históricos de estado de los certificados, o en caso contrario, validez de los certificados en el momento de la validación: certificados no revocados, suspendidos, o que hayan expirado, y la validación de la cadena de certificación (incluida la validación de todos los certificados de la cadena). Esta información puede estar contenida en la propia firma en el caso de las firmas longevas.
3. Certificado expedido bajo una Declaración de Prácticas de Certificación específica.
4. Verificación, si existen y si así lo requiere la plataforma de relación electrónica o un servicio concreto de dicha plataforma, de los sellos de tiempo de los formatos implementados, incluyendo la verificación de los periodos de validez de los sellos. Si alguna de estas verificaciones es errónea, el proceso de firma se interrumpirá. Si no fuese posible realizar estas comprobaciones en el momento de la firma, será necesario, en todo caso, que los sistemas receptores de la firma asuman dicha validación, antes de aceptar el fichero, formulario u otro objeto binario firmado.

2. Reglas comunes para la validación de una firma electrónica

Para garantizar la validez de los documentos con firma electrónica de que se haga uso en sus procedimientos utilizará algunos de estos sistemas o procesos:

- @firma: plataforma de validación de certificados y firmas electrónicas.
- VALIDe: Aplicación web de acceso libre para la validación de firmas y certificados online, así como demostrador de servicios de @firma. https://valide.redsara.es/valide/inicio.html
- Herramienta web de acceso libre para validación de firmas y certificados de la Comisión Europea: https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation
- Mediante la comprobación en sede electrónica del organismo emisor del documento del código seguro de verificación (CSV) en los casos que sea de aplicación.

En caso de producirse algún problema técnico o dificultad administrativa que imposibilitase la validación de la firma electrónica con los mecanismos señalados anteriormente, se podrá utilizar de manera excepcional el siguiente proceso de validación:

- Se verificará en primer lugar la inexistencia de errores a través de la herramienta que incluya el visor de pdf, establecido como software corporativo en Enresa.
- Si no existen errores de verificación, a continuación, se comprobará que la firma electrónica se ha realizado con un certificado cualificado expedido por un proveedor de servicios de certificación de confianza cualificado, acreditando que se encuentra publicado en la lista de confianza de proveedores de servicios de certificación supervisados de los estados miembros de la Unión Europea, a través de la web:
  https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

Debiendo identificar el servicio de confianza asociado a la firma en el archivo, comprobándose al menos, la correspondencia de su identidad digital y de la política de la extensión.

Esta política fue aprobada y firmada por el
Consejo de Administración de Enresa en su sesión del 26 de junio de 2023